**УДК 338** **DOI: 10.34670/AR.2020.85.71.047**

# Компьютерная безопасность: анализ современных видов кибератак и пути их преодоления

**Михайлов Алексей Витальевич**

Независимый эксперт,
119019, Российская Федерация, Москва, ул. Воздвиженка, 3/5;
e-mail: alexey.mihailov94@mail.ru

**Аннотация**

Статья посвящена обзору современных видов кибератак, распространенных во всем мире, и возможных способов их преодоления. Проведенное исследование позволяет утверждать, что отрасль информационных технологий вынуждена находиться в состоянии повышенной готовности на фоне множества новых развивающихся угроз кибербезопасности, а «эпидемия» киберпреступности может поставить под сомнение общественную веру в сохранность личной информации и конфиденциальности. В настоящее время кибератаки на компании и отдельные лица кажутся неизбежными, но в большинстве случаев их можно избежать, если выполнять приведенные в данной статье рекомендации.

В работе показано, что целесообразно инвестировать в страхование кибербезопасности. Киберпреступники стали крайне искушенными и способны проникнуть в самые передовые средства кибербезопасности, поэтому даже наиболее защищенные компании становятся уязвимыми для кибератак. Именно в подобных случаях важно страхование кибербезопасности. Если происходит кибератака, большинство страховых компаний не только покрывают финансовые потери, вызванные кражей данных, но также помогают совместно оплачивать расходы, связанные с восстановлением данных, включая оплату услуг экспертов по восстановлению данных и покупки нового оборудования и программного обеспечения.

В работе показано, что целесообразно инвестировать в страхование кибербезопасности. Киберпреступники стали крайне искушенными и способны проникнуть в самые передовые средства кибербезопасности, поэтому даже наиболее защищенные компании становятся уязвимыми для кибератак. Именно в подобных случаях важно страхование кибербезопасности. Если происходит кибератака, большинство страховых компаний не только покрывают финансовые потери, вызванные кражей данных, но также помогают совместно оплачивать расходы, связанные с восстановлением данных, включая оплату услуг экспертов по восстановлению данных и покупки нового оборудования и программного обеспечения.

**Для цитирования в научных исследованиях**

Михайлов А.В. Компьютерная безопасность: анализ современных видов кибератак и пути их преодоления // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 4А. С. 398-405. DOI: 10.34670/AR.2020.85.71.047

**Ключевые слова**
Компьютерная безопасность; киберпреступность; кибербезопасность; кибератаки.

## Введение

В настоящее время отрасль информационных технологий вынуждена находиться в состоянии повышенной готовности на фоне множества новых развивающихся угроз кибербезопасности. Все более изощренные кибератаки, связанные с вредоносными программами, фишингом, машинным обучением, искусственным интеллектом, криптовалютой и многим другим, подвергают данные и активы корпораций, правительств и отдельных лиц постоянному риску.

Отрасль информационных технологий столкнулась с проблемой острой нехватки специалистов по кибербезопасноти, следовательно, «эпидемия» киберпреступности может поставить под сомнение общественную веру в сохранность личной информации и конфиденциальности.

## Основное содержание

Некоммерческий Форум по информационной безопасности, описывающий себя как «ведущий мировой авторитет в области кибербезопасности, информационной безопасности и управления рисками», в своем ежегодном исследовании «Threat Horizon» отмечает увеличение потенциала следующих направлений развития кибератак:

Сбои – чрезмерная зависимость от подверженных рискам подключений создает возможность преднамеренных перебоев в работе Интернета, способных отрицательно сказаться на сфере торговли, и повышает риск того, что вредоносные программы, требующие выкуп, будут использоваться для кражи технологий «Интернет вещей»;

Искажения – преднамеренное распространение дезинформации, в том числе с помощью ботов и автоматических источников, ставит под угрозу доверие к целостности информации;

Повреждения – быстрое развитие интеллектуальных технологий в дополнение к противоречивым требованиям, возникающим в связи с развитием национальной безопасности и индивидуальных правил конфиденциальности, негативно влияет на способность организаций контролировать имеющуюся собственную информацию.

По прогнозам компании «Cybersecurity Ventures», являющейся ведущей мировой компанией по исследованиям и разработкам в сфере глобальной киберэкономики, ущерб, связанный с киберпрестпуностью, к 2021 году достигнет 6 трлн. долларов США.

Следует рассмотреть следующие виды кибератак в качестве основных угроз и тенденций кибербезопасности в 2020 году.

Фишинг становится все более изощренным и сложным для предотвращения. Фишинговые атаки, при которых людям передаются строго предназначенные цифровые сообщения, вынуждают пользователей переходить по ссылке, которая может установить вредоносное программное обеспечение или раскрыть конфиденциальные данные.

В настоящее время, когда сотрудники большинства организаций осведомлены об опасностях фишинга электронной почты или перехода по подозрительным ссылкам, хакеры

используют машинное обучение для гораздо более быстрого создания и распространения убедительных фальшивых сообщений в надежде, что получатели невольно скомпрометируют компьютерные сети и системы своей организации. Такие атаки позволяют хакерам украсть логины пользователей, учетные данные кредитных карт и другие виды личной финансовой информации, а также получить доступ к частным базам данных.

Атаки программ-вымогателей каждый год приносят ущерб в миллиарды долларов США, поскольку хакеры внедряют технологии, которые позволяют им буквально похищать базы данных отдельных лиц или организаций и хранить всю информацию для получения выкупа. Рост популярности криптовалют, таких как Bitcoin, объясняется тем, что он помогает вымогателям совершать свои атаки, позволяя анонимно оплачивать требования выкупа.

Некоторые эксперты считают, что, поскольку компании продолжают концентрировать усилия на создание более надежной защиты от взломов вымогателей, хакеры будут все чаще нацеливаться на других потенциально прибыльных жертв, к примеру, людей с высоким уровнем дохода.

Криптоджекинг является еще одной современной формой кибератаки, возникшей на фоне движения криптовалюты, также влияющей на кибербезопаснсоть. Криптоджекинг представляет собой новую тенденцию, при которой киберпреступники похищают чужие домашние или рабочие компьютеры для майнинга криптовалюты. Принимая во внимание тот факт, что для майнинга требуются огромные вычислительные мощности, хакеры могут зарабатывать деньги, тайно привязываясь к чужим системам. Для предприятий, столкнувшихся с криптоджекингом, могут возникнуть серьезные проблемы, связанные с производственным процессом или с дорогостоящим временем простоя оборудования, пока ИТ-специалисты будут пытаться выследить и решить возникшую проблему.

В качестве еще одной кибератаки, несущей в себе риск, можно выделить кибер-физические атаки, представляющие собой ту же технологию, которая позволила модернизировать и компьютеризировать критически важные сегменты инфраструктуры. Сохраняющаяся угроза хакерских атак на электрические сети, транспортные системы, водоочистные сооружения и т.д. представляет собой серьезную уязвимость в будущем. Согласно последнему отчету газеты «The New York Times», американские многомиллиардные военные системы также подвергаются риску преступных атак на основе высоких технологий.

Помимо хакеров, стремящихся получить прибыль за счет кражи индивидуальных и корпоративных данных, целые государства сегодня используют свои кибервозможности для проникновения в системы других государств и осуществления атак на критически важные сферы инфраструктуры. В настоящее время киберпреступность представляет собой серьезную угрозу не только для частного сектора и отдельных лиц, но и для правительств и целых государств. В 2020 году следует ожидать усиления спонсируемых государством атак, в частности на особо важные объекты, что с каждым годом вызывает все большую озабоченность.

Многие подобные атаки направлены на государственные системы и инфраструктуру, но и организации частного сектора могут быть подвержены такому риску. Согласно отчету компании «Thomson Reuters Labs», кибератаки, спонсируемые государством, представляют собой развивающийся и значительный риск для частного предпринимательства, бросающего новые вызовы тем секторам делового мира, которые обеспечивают подходящие цели для урегулирования геополитических вопросов.

Атаки на основе технологии «Интернет вещей» (Internet of Things – IoT), которая представляет собой концепцию вычислительной сети физических предметов, имеющих встроенные технологии для взаимодействия друг с другом или с внешней средой, с каждым днем становятся все более распространенными, и, согласно данным Интернетресурса Statista.com, к 2025 году число устройств, подключенных к IoT, достигнет 75 миллиардов. В число IoT входят ноутбуки, планшеты, маршрутизаторы, веб-камеры, бытовая техника, умные часы, медицинские приборы, производственное оборудование, автомобили и системы домашней безопасности.

Технология IoT удобна для потребителей, и многие компании в настоящее время используют ее для экономии денег, собирая при этом огромные объемы ценных данных и оптимизируя бизнес-процессы. Однако большее количество подключенных друг к другу устройств означает больший риск и большую уязвимость для кибератак и вирусов. Контролируемые хакерами устройства IoT могут использоваться для создания отрицательных воздействий, перегрузки сетей или блокировки необходимого оборудования для получения финансовой выгодны.

Индустрия здравоохранения переживает серьезную эволюцию, поскольку большинство медицинских карт пациентов в настоящее время перешли в онлайн формат, и медицинские работники осознают преимущества усовершенствованных интеллектуальных медицинских устройств и электронных медицинский карт. Однако, поскольку индустрия здравоохранения приспосабливается к цифровому веку, возникает ряд проблем, связанных с угрозами конфиденциальности и кибербезопасности.

По данным Института разработки программного обеспечения Университета Карнеги-Меллона, чем больше устройств будет подключено к сетям больниц и медицинских учреждений, тем данные и информации о пациентах буду становиться все более уязвимыми. Особое беспокойство вызывает риск удаленного взлома устройства, напрямую подключенного к пациенту. Злоумышленник теоретически может увеличить или уменьшить дозу лекарств, посылать электрические сигналы пациенту или отключить мониторинг показателей жизнедеятельности.

Учитывая, что больницы и медицинские учреждения все еще адаптируются к цифровому оформлению медицинских карт пациентов, хакеры используют множество уязвимых мест в средствах их защиты. Сегодня, когда медицинские записи пациентов почти полностью переведены в формат онлайн, они являются главной целью хакеров из-за секретной информации, которую они содержат.

Третьи стороны, такие как поставщики и подрядчики, представляют огромный риск для компаний, большинство из которых не имеют защищенной системы или специальной группы для управления сторонними сотрудниками.

По мере того, как киберпреступники становятся все более изощренными, а угрозы кибербезопасности продолжают расти, организации в большей мере осознают потенциальную угрозу, создаваемую третьими сторонами. Тем не менее, риск по-прежнему остается очень высоким, к примеру, Таможенная и пограничная служба США присоединились к списку резонансных случаев кибератак в 2019 году.

Согласно отчету «Угрозы безопасности для отношений со сторонними поставщиками», опубликованный Интернет-ресурсом

RiskManagementMonitor.com, 60% взломов данных связаны с третьей стороной, и только 52% компаний имеют стандарты безопасности в отношении сторонних поставщиков и подрядчиков.

Подключенные автомобили и полуавтономные транспортные средства используют встроенные датчики для оптимизации своей работы и комфорта пассажиров. Автомобили и транспортные средства обычно подключаются с помощью встроенного, привязанного или интегрированного смартфона. По мере развития технологий подключенный автомобиль становится все более распространенным явлением. В 2020 году примерно 90% новых автомобилей буду подключены к Интернету, согласно отчет «7 тенденций в области подключенных автомобилей, которые способствую будущему».

Для хакеров подобная эволюция в производстве и дизайне автомобилей означает еще одну возможность использования уязвимостей в небезопасных системах и кражи конфиденциальных данных. Таким образом, в дополнение к проблемам безопасности, подключенные автомобили создают серьезные проблемы конфиденциальности.

По мере того, как производители стремятся выйти на рынок с высокотехнологичными автомобилями, в 2020 году прогнозируется увеличение не только количества подключенных автомобилей, но и количества и серьезность обнаруженных уязвимых мест в системах.

Киберпреступники постоянно совершенствуются не только в использовании технологий, но и в психологии. Компания, предоставляющая услуги по кибербезопаснсоти, «Tripwire» описывает социальных инженеров как хакеров, которые используют одно единственное уязвимое место, которое имеется в каждой организации, а именно человеческую психологию. Используя различные средства массовой информации, включая телефонные звонки и социальные сети, злоумышленники обманывают людей, предлагая им доступ к конфиденциальной информации.

«Эпидемия» киберпреступности в последние годы быстро обострилась, в то время как компании и правительства изо всех сил пытались нанять достаточное количество квалифицированных специалистов для защиты от растущей угрозы. Следует ожидать, что подобная тенденция сохранится и после 2020 года, при этом, по некоторым оценкам, нехватка специалистов по кибербезопасности в мире составляет около 1 миллиона (данный показатель потенциально возрастет до 3,5 миллиона к 2021 году).

Серьезная нехватка квалифицированных специалистов в области кибербезопасности по-прежнему вызывает тревогу, поскольку сильная и высококвалифицированная цифровая рабочая сила необходима для борьбы с более частыми, более изощренными угрозами кибербезопаснсоти, исходящими со всего мира.

Серьезные кибератаки повысили осведомленность о растущей угрозе киберпреступности. Недавние опросы, проведенные компаниями «Small Business Authority», «Symantec», Лабораторией Касперского и Национальным альянсом по кибербезопасности, показывают, что многие топ-менеджеры и владельцы компаний все еще имеют ложное представление о кибербезопасности.

Подавляющее большинство малых и средних предприятий США не имеют официальной политики безопасности в Интернете для своих сотрудников, и только около половины имеют самые элементарные меры по кибербезопасности. Кроме того, только около четверти владельцев малого бизнеса провели сторонние испытания своих компьютерных систем, для того

чтобы убедиться, что они защищены от хакерских атак, и почти 40% не имеют резервных копий своих данных, хранящихся в более чем одном месте.

Несмотря на значительные риски кибербезопасности, 85% владельцев малого и среднего бизнеса считают, что их компании защищены от хакеров, вирусов, вредоносных программ или взлома данных. Высокий показатель в значительной степени связан с широко распространенным, хотя и ошибочным, убеждением, что малые предприятия, скорее всего, не станут объектами кибератак. В действительности хакеры просто ищут пути наименьшего сопротивления, а 40% атак направлены против организаций с числом сотрудников менее 500 человек.

Внешние источники, такие как хакеры, являются не единственным способом атаки на компанию. В небольших компаниях чаще всего царит доверительная атмосфера, но именно это может стать уязвимым место для атак.

По мере того, как крупные компании продолжают серьезно относиться к безопасности данных, малые предприятия становятся все более привлекательными целями, а результаты зачастую бывают разрушительными.

## Заключение

Несмотря на то, что в настоящее время у многих компаний нет ресурсов для привлечения стороннего эксперта для проверки компьютерных систем и разработки рекомендаций по обеспечению безопасности, можно предпринять простые и экономичные шаги, для того чтобы снизить риск кибератаки:

– Обучить сотрудников принципам кибербезопасности.
– Установить, использовать и регулярно обновлять антивирусное программное обеспечение на каждом компьютере, которые используется в компании.
– Использовать брандмауэр для подключения к Интернету.
– Загружать и устанавливать обновления программного обеспечения для операционных систем и приложений по мере их появлений.
– Создавать резервные копии важных бизнес-данных и информации.
– Контролировать физический доступ к компьютерам и сетевым компонентам.
– Защищать сети Wi-Fi, они должны быть безопасными и скрытыми.
– Создавать индивидуальные учетные записи пользователей для каждого сотрудника.
– Ограничить доступ сотрудника к данным и информации и ограничить полномочия на установку программного обеспечения.
– Регулярно менять пароль.

Кроме того, целесообразно инвестировать в страхование кибербезопасности. Киберпреступники стали крайне искушенными и способны проникнуть в самые передовые средства кибербезопасности, поэтому даже наиболее защищенные компании становятся уязвимыми для кибератак. Именно в подобных случаях важно страхование кибербезопасности. Если происходит кибератака, большинство страховых компаний не только покрывают финансовые потери, вызванные кражей данных, но также помогают совместно оплачивать расходы, связанные с восстановлением данных, включая оплату услуг экспертов по восстановлению данных и покупки нового оборудования и программного обеспечения.

В настоящее время кибератаки на компании и отдельные лица кажутся неизбежными, но в

большинстве случаев этих атак можно избежать, если выполнять вышеприведенные советы и ряд действий, специально разработанных для защиты предприятий от хакеров.

## Библиография

1. Bisson D. 5 Social Engineering Attacks to Watch Out For // Tripwire. [Электронный ресурс]. – Режим доступа: https://www.tripwire.com/state-of-security/security-awareness/5-socialengineering-attacks-to-watch-out-for/
2. Internet of Things - number of connected devices worldwide 2015-2025 published by Statista Research Department. [Электронный ресурс]. – Режим доступа: https://www.statista.com/statistics/471264/iot-numberof-connected-devices-worldwide/
3. King C. 10 At-Risk Emerging Technologies // Software Engineering Institute of Carnegie Mellon University. [Электронный ресурс]. – Режим доступа: https://insights.sei.cmu.edu/sei_blog/2016/05/10-atrisk-emerging-technologies.html
4. McDonald C. Security Risks of Third-Party Vendor Relationships // Risk Management Monitor. [Электронный ресурс]. – Режим доступа: https://www.riskmanagementmonitor.com/security-risks-of-third-partyvendor-relationships/
5. Morgan S. Cybercrime Damages $6 Trillion By 2021 // Cybercrime Magazine. [Электронный ресурс]. – Режим доступа: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report2016/
6. Morgan S. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021 // Cybercrime Magazine. [Электронный ресурс]. – Режим доступа: https://cybersecurityventures.com/jobs/
7. Morley C. 7 Connected Car Trends Fueling the Future // Medium. [Электронный ресурс]. – Режим доступа: https://medium.com/iotforall/7-connected-car-trends-fueling-the-future946b05325531
8. Sanger D., Broad W. New U.S. Weapons Systems Are a Hackers' Bonanza, Investigators Find // The New York Times. [Электронный ресурс]. – Режим доступа: https://www.nytimes.com/2018/10/10/us/politics/hackers-pentagonweapons-systems.html
9. Significant Cyber Incidents by Center for Strategic and International Studies. [Электронный ресурс]. – Режим доступа: https://www.csis.org/programs/technology-policy-program/significantcyber-incidents
10. Ulicny B. Today's enterprises face increasing risk of state-sponsored cyberattacks // Thomson Reuters. [Электронный ресурс]. – Режим доступа: https://blogs.thomsonreuters.com/answerson/state-sponsoredcyberattacks/

# Computer security: analysis of modern types of cyber attacks and ways to overcome them

**Aleksei V. Mikhailov**

Independent researcher,
119019, 3/5 Vozdvizhenka str., Moscow, Russian Federation;
e-mail: alexey.mihailov94@mail.ru

**Abstract**

The article is devoted to the review of modern types of cyber attacks that are common all over the world, and possible ways to overcome them. The study suggests that the information technology industry is forced to be on high alert against the backdrop of many new emerging threats to cybersecurity, and the "epidemic" of cybercrime may call into question public confidence in the safety of personal information and privacy. Currently, cyber attacks on companies and individuals seem inevitable, but in most cases they can be avoided if you follow the recommendations in this article.

The paper shows that it is advisable to invest in cybersecurity insurance. Cybercriminals have become extremely sophisticated and able to penetrate the most advanced means of cybersecurity, so even the most secure companies become vulnerable to cyber attacks. It is in such cases that

cybersecurity insurance is important. If a cyber attack occurs, most insurance companies not only cover financial losses caused by data theft, but also help pay the costs of data recovery together, including paying for the services of data recovery experts and the purchase of new hardware and software.

**For citation**

Mikhailov A.V. (2020) Komp'yuternaya bezopasnost': analiz sovremennykh vidov kiberatak i puti ikh preodoleniya [Computer security: analysis of modern types of cyber attacks and ways to overcome them]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 10 (4A), pp. 398-405. DOI: 10.34670/AR.2020.85.71.047

**Keywords**

Computer security; cybercrime; cybersecurity; cyber attacks.

## References

1. Bisson D. 5 Social Engineering Attacks to Watch Out For // Tripwire. [Electronic resource]. - Mode of access: https://www.tripwire.com/state-of-security/security-awareness/5-socialengineering-attacks-to-watch-out-for/
2. Internet of Things - number of connected devices worldwide 2015-2025 published by Statista Research Department. [Electronic resource]. - Mode of access: https://www.statista.com/statistics/471264/iot-numberof-connected-devices-worldwide/
3. King C. 10 At-Risk Emerging Technologies // Software Engineering Institute of Carnegie Mellon University. [Electronic resource]. - Mode of access: https://insights.sei.cmu.edu/sei_blog/2016/05/10-atrisk-emerging-technologies.html
4. McDonald C. Security Risks of Third-Party Vendor Relationships // Risk Management Monitor. [Electronic resource]. - Mode of access: https://www.riskmanagementmonitor.com/security-risks-of-third-partyvendor-relationships/
5. Morgan S. Cybercrime Damages $6 Trillion By 2021 // Cybercrime Magazine. [Electronic resource]. - Mode of access: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report2016/
6. Morgan S. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021 // Cybercrime Magazine. [Электронный ресурс]. – Режим доступа: https://cybersecurityventures.com/jobs/
7. Morley C. 7 Connected Car Trends Fueling the Future // Medium. [Electronic resource]. - Mode of access: https://medium.com/iotforall/7-connected-car-trends-fueling-the-future946b05325531
8. Sanger D., Broad W. New U.S. Weapons Systems Are a Hackers' Bonanza, Investigators Find // The New York Times. [Electronic resource]. - Mode of access: https://www.nytimes.com/2018/10/10/us/politics/hackers-pentagonweapons-systems.html
9. Significant Cyber Incidents by Center for Strategic and International Studies. [Electronic resource]. - Mode of access: https://www.csis.org/programs/technology-policy-program/significantcyber-incidents
10. Ulicny B. Today's enterprises face increasing risk of state-sponsored cyberattacks // Thomson Reuters. [Electronic resource]. - Mode of access: https://blogs.thomsonreuters.com/answerson/state-sponsoredcyberattacks/